*A*udit

*R*eport

SUMMARY OF AUDITS OF
ACQUISITION OF INFORMATION TECHNOLOGY

Report No. D-2000-162   July 13, 2000

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

<div align="center">

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

</div>

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

GAO	General Accounting Office
IG	Inspector General
MAIS	Major Automated Information System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON. VIRGINIA 22202

July 13, 2000

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)

SUBJECT: Audit Report on a Summary of Audits of Acquisition of Information
Technology (Report No. D-2000-162)

We are providing this report for your information and use.   Because this report
contains no recommendations, no written comments were required, and none were
received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the audit staff. For additional
information on this report, please contact Mr. John A. Mitton at (703) 604-9019
(DSN 6649019) (jmitton@dodig.osd.mil) or Mr. Charles M. Santoni at
(703) 604-9051 (DSN 664-9051) (csantoni@dodig.osd.mil). See Appendix C for the
report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Report No. D-2000-162   **July 13, 2000**
(Project No. D2000AL-0166.00)

Summary of Audits of Acquisition of Information Technology

Executive Summary

Introduction. In the DoD Appropriations Act for FY 2000, Congress reemphasized the need for effective implementation of oversight processes associated with the Clinger-Cohen Act of 1996. This act calls for an investment oversight process that covers the life of each system and includes explicit criteria for analyzing projected and actual costs, benefits, and risks associated with the investments. DoD has approximately 5,800 mission-critical or mission-essential information technology systems. Of these, 71 are categorized as Major Automated Information Systems.

Information technology comprises any equipment or interconnected subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This report summarizes 30 audit reports that address the acquisition of information technology within the DoD. We summarized reports issued from October 1, 1996, through March 31, 2000. Of these, 17 were prepared by the Inspector General, DoD, 4 were prepared by the General Accounting Office, and 9 were prepared by the Service audit agencies.

Objectives. The overall objective was to summarize the results of 30 audit reports that discussed acquisition of information technology and identify systemic issues addressed by the reports.

Results. Acquiring information technology in accordance with Congressional direction and Office of Management and Budget and DoD guidance continues to challenge DoD. Our analysis of 30 reports (see Appendix B) shows that the economy and efficiency with which information technology is acquired varies greatly among DoD organizations. Within these 30 reports, systemic problems were identified in the following areas:

- inadequate documentation/validation of the system requirements (13 reports),

- inaccurate life-cycle cost analysis or incomplete cost data (9 reports),

- incomplete analysis of alternatives to assure that programs are not duplicative and are most cost effective (8 reports),

- systems not properly categorized for oversight purposes according to the acquisition criteria established in DoD policy (7 reports), and

- incomplete or nonexistent acquisition program baselines to record cost, schedule and performance goals (7 reports).

Further, recurring problems existed in the areas of inadequate system testing, schedule slippage, and the lack of an implementation strategy. Each of these problems was noted in three reports. As a result of these systemic and recurring management oversight weaknesses, DoD is acquiring information technology that may not meet the needs of the user, which makes it difficult to meet performance measures; whose true costs are unknown, which makes it difficult to assess return on investment; and that may duplicate existing systems, which is contrary to Congressional direction and the DoD policy of portfolio management.

DoD is attempting to provide the critical management oversight controls called for in the Clinger-Cohen Act and the FY 2000 DoD Appropriations Act by instituting a program of information technology portfolio management. Adequate implementation of portfolio management by DoD, to include establishment of the necessary internal management controls by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), is intended to reduce the instances of the problems noted. Details of the results can be found in the finding section of this report.

Management Comments. We provided a draft of this report to management on May 26, 2000. Because the draft report contained no recommendations, written comments were not required, and none were received. Therefore, we are publishing this report in final form.

Table of Contents

Background

According to the Clinger-Cohen Act of 1996, formerly known as the Information Technology Management Reform Act of 1996, information technology comprises any equipment, or interconnected subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The act requires the establishment of an investment oversight process for analyzing, tracking, and evaluating the risks and results of all major capital investments made for information technology and covers the life of each system including explicit criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments. The Clinger-Cohen Act also requires that before investing in information technology, agencies should analyze the function associated with the new acquisition to determine if this function could be made more efficient or would be better performed by the private sector. In 1998, DoD established an information technology functional area reform goal to institutionalize provisions of the Clinger-Cohen Act and provide services that satisfy customer information needs.

Office of Management and Budget Guidance

Office of Management and Budget Circular No. A-11, Part Three, "Planning, Budgeting, and Acquisition of Capital Assets," 1999, provides guidance for implementing the Clinger-Cohen Act. This circular emphasizes the need for realistic cost, schedule, and performance baselines. The circular requires constant monitoring of actual work performed against the baselines that should be used to revise estimates of cost, schedule, and performance as appropriate.

Office of Management and Budget Circular A-109. "Major Systems Acquisitions," April 1976, provides policies for the acquisition management of major systems. The circular requires that acquisition programs maintain capabilities to:

- predict, review, assess, negotiate, and monitor program costs;

- assess acquisition cost, schedule, and performance experience against predictions, and report on such assessments;

- make new assessments where significant cost, schedule, or variances occur;

- estimate life-cycle costs during system design-concept evaluation and update cost estimates throughout the acquisition life cycle to evaluate appropriate trade-offs among investment costs, ownership costs, schedules and performances; and

- use independent cost estimates for comparisons, where feasible.

1

Office of Management and Budget Circular A-123, "Management Accountability and Control," June 1995, implements the Federal Manager's Financial Integrity Act of 1982. The circular defines management controls as the organization, policies, and procedures used to reasonably ensure that programs achieve their intended results; resources are consistent with the agency mission; programs are protected from waste, fraud, and mismanagement; laws and regulations are followed; and reliable and timely information is obtained, maintained, reported, and used for decisionmaking. Further, the circular requires management controls to be an integral part of the mission area, planning, budgeting, management, accounting, and auditing cycles.

DoD Policy

DoD Directive 5000.1, "Defense Acquisition," March 15, 1996, implements Office of Management and Budget Circulars A-109 and A-123 and was modified to reflect requirements from the Clinger-Cohen Act. The directive states that the primary objective of the defense acquisition system is to acquire quality products that satisfy the needs of operational users with measurable improvements to mission accomplishments, in a timely manner, and at a fair and reasonable price. The directive emphasizes the importance of rigorous internal controls with control objectives for cost, schedule, and performance parameters embodied in acquisition program baselines. Also, the directive provides the basic criteria for defining an information technology acquisition program as a Major Automated Information System (MAIS). A MAIS is any program so designated by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) or estimated to require program costs in any single year in excess of $30 million in FY1996 constant dollars, total program costs in excess of $120 million in FY1996 constant dollars, or total life-cycle costs in excess of $360 million in FY1996 constant dollars. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) has the ultimate oversight responsibility for MAIS programs.

Congressional Direction and DoD Corrective Action

The House Appropriations Committee Report 105-591 that accompanied the DoD Appropriations Act for FY 1999, reflected Congressional concern about the adequacy of DoD oversight of its information technology systems. Specifically, Congress required that most information technology acquisitions be categorized as investments to be financed with procurement or research, development, test, and evaluation funds as opposed to operations and maintenance funds. As a corrective action, the Under Secretary of Defense (Comptroller) issued policy that clarifies procedures for funding information technology systems.

In the Conference Report for the DoD Appropriations Act for FY 2000, Congress expressed continued concern with DoD acquisition practices for information technology and reemphasized the importance of the Clinger-Cohen Act by requiring that all 71 MAISs be certified as being developed in accordance with the Clinger-Cohen Act prior to being approved to the next

milestone level. The DoD Chief Information Officer must provide those certifications to Congress. Also, the Conference Report to the Appropriations Act requires that the approximately 5,800 mission-critical and mission-essential information technology systems be registered with the DoD Chief Information Officer.

To establish the management controls necessary to comply with the Clinger-Cohen Act and subsequent Congressional direction and Office of Management and Budget guidance, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is beginning to implement the portfolio management concept. This oversight concept, managed by the DoD Chief Information Officer, requires that information technology investment decisions be directly linked to DoD mission, warfighter, and functional goals, and outcomes. Information technology investments must result in measurable improvements to DoD mission-related and administrative processes, and processes and systems must be certified as compliant with the Clinger-Cohen Act and any related reform legislation.

A portfolio will be the group of capabilities, resources, management, and related investments that are required to accomplish a mission-related or administrative outcome. One of the principal features of portfolio management is the establishment of an Overarching Integrated Product Team which will develop and implement procedures to provide visibility in investments to ensure that managing procedures are in accordance with the Clinger-Cohen Act. A key feature of portfolio management is the performance of mission analysis in which principal staff assistants, Joint Staff, and Components determine mission area warfighter, business, and administrative needs, formulate strategic plans and goals to meet those needs, identify performance gaps and opportunities, and provide a performance based plan to fulfill the mission area needs. DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs," March 15, 1996, is undergoing revision to require the use of portfolio management.

Inspector General, DoD, Testimony

For several years, in semiannual reports to Congress and testimony, the Inspector General, DoD, (IG, DoD) has emphasized the weakness in the acquisition of information technology. For example, on February 25, 1999, the IG, DoD, testified before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, United States House of Representatives, on DoD vulnerabilities to fraud, waste, and abuse. The IG, DoD, stated that DoD faces major problems related to the acquisition of information technology and has categorized the acquisition of information technology as one of 10 high-risk areas for DoD because information technology acquisition projects have tended to overrun budgets, evade data standardization and interoperability requirements, and shortchange user needs. The IG, DoD, noted that audits have indicated that cost, schedule, and performance baselines are not always established for information technology development projects. The chart on page 8 is a matrix of General Accounting Office (GAO), IG, DoD, and Service audit agency reports relating to

information technology acquisition weaknesses. Of the 30 reports issued from October 1, 1996, until March 31, 2000, 17 reports were issued by the IG, DoD, 4 by GAO, and 9 by the Service audit agencies.

Objectives

The overall objective was to summarize the results of 30 audit reports that discussed acquisition of information technology and identify systemic issues addressed by the report. See Appendix A for the discussion of the scope. Appendix B contains a summary of each report and the corrective action taken.

Information Technology Acquisition

Acquiring information technology in an efficient and economical manner continues to challenge DoD. Review of 30 reports (see Appendix B) disclosed that the economy and efficiency with which information technology is acquired varies greatly among DoD organizations. Within these 30 reports, systemic problems were identified in the following areas:

- inadequate documentation/validation of the system requirements (13 reports),

- inaccurate life-cycle cost analysis or incomplete cost data (9 reports),

- incomplete analysis of alternatives to assure that programs are not duplicative and are most cost effective (8 reports).

- systems not properly categorized for oversight purposes according to the acquisition criteria established in DoD policy (7 reports), and

- incomplete or nonexistent acquisition program baselines to record schedule and performance goals (7 reports).

While not systemic, there were recurring problems in the areas of inadequate system testing, schedule slippage, and the lack of an implementation strategy. Each of these problems was noted in three reports. These systemic and recurring problems resulted from lack of program management attention to detail and failure of overall DoD oversight management controls to enforce policies designed to ensure sound business practices such as accurate preparation of and adherence to costs, schedule, and performance baselines. As a result of these systemic and recurring management oversight weaknesses, DoD is acquiring information technology that may not meet the needs of the user, which makes it difficult to meet performance, whose true costs are unknown, which makes it difficult to assess return on investment; measures; and that may duplicate existing systems, which is contrary to Congressional direction and the DoD policy of portfolio management.

Documentation/Validation of System Requirements. Thirteen of the information technology acquisition reports noted inadequate documentation or validation of system requirements. For the Audit of "Requirements Planning and Impact on Readiness of Training Simulators and Devices," we raised concern that the Joint Requirements Oversight Council process was not properly used to validate the requirements for two systems; thus, resulting in the acquisition of two seemingly duplicative systems. Similarly, due to a failure to adequately validate requirements, the Defense Logistics Agency Electronic Catalog Pilot Program is partially duplicative of a General Services Administration program. The Standard Procurement System needed additional refinements to meet user needs and to standardize procurement policies, processes, and procedures. We found that 13 of 25 fielded sites for the Standard

Procurement System were not using the system because critical system functions were either not included in the initial versions of the system or were not functioning. The Air Force Audit Agency found that 6 of 12 automated intelligence information systems that were reviewed did not document the need for the system. The Army Audit Agency found that user requirements were neither identified nor satisfied in the acquisition of the Army's portion of the Global Command and Control System. The GAO found that the Army developed digitized battlefield systems without testing to assure that the requirement to combat the threat of command and control warfare attacks was satisfied. Failure to properly document and validate requirements increases the risk of developing systems that fail to meet the needs of intended users or waste funds by duplicating existing systems (see Appendix B, reports 1, 5, 9, 11, 13, 14, 21, 22, 23, 24, 25, 26, 27).

Life-cycle Cost Analysis or Cost Data. Nine of the information technology acquisition reports summarized in Appendix B note that system life-cycle cost analyses were either inaccurate or that cost data was incomplete. For example, the program management for the Joint Total Asset Visibility System did not establish cost baselines; therefore, variances could not be analyzed and budget submissions were not verified. For the Composite Health Care System II, cost baselines were not established and funding was combined with that of other systems making it difficult to determine system cost. The Air Force failed to establish the proper management controls to provide for accurate life-cycle costing for the Defense Civilian Personnel Data System. The life-cycle costs for the Corporate Executive Information System and the Defense Security Assistance Management System were not adequately estimated; therefore, these systems were not categorized as MAIS and did not receive appropriate oversight although they should have been categorized as such. GAO identified a general pattern within DoD of failure to perform the accurate cost calculations to determine return on investment. Without accurate cost data, it is difficult, at best, to properly budget for and categorize systems during development thus risking the development of high-cost systems without proper oversight (see Appendix B, reports 3, 4, 9, 12, 14, 19, 21, 24, 30).

Analysis of Alternatives. Eight reports noted problems with the Analysis of Alternatives. The GAO found that the lack of independent verification of Analysis of Alternatives was a widespread problem and that DoD was automating functions that were planned for outsourcing. We found that the Defense Logistics Agency Electronic Catalog Pilot Program was duplicative of General Service Administration efforts, and no clear Analysis of Alternatives was undertaken for the Joint Accounting System Initiative. The Air Force Audit Agency found that alternatives were not considered in replacing computers versus the less costly upgrade of older computers. An Analysis of Alternatives is important to assure that prior to developing a new system there are not less costly acceptable alternatives to the new development (see Appendix B, reports 10, 17, 21, 22, 23, 26, 27, 30).

Acquisition Categorization. Seven of the information technology acquisition reports noted that systems were not placed in the proper acquisition category for proper oversight as defined in DoD Directive 5000.1, "Defense Acquisition," March 15, 1996. This issue is closely related to the prior issue of inadequate life-cycle cost analysis and cost data. Had adequate cost data and projections

been available, it would have been more obvious that these systems were miscategorized. These reports identify five systems that should have been categorized as a MAIS but were not. The five systems are the Corporate Executive Information System, the Defense Security Assistance Management System, the Joint Intelligence Virtual Architecture, the Training Simulators and Devices, and the Joint Total Asset Visibility System. Miscategorization results in significant expenditures of funds without the required oversight processes being implemented, thus risking program failure of systems that have expended considerable funds. Miscategorization is also often a root cause associated with failure to establish acquisition program baselines, and calculate accurate life-cycle cost data (see Appendix B, Reports 4, 6, 12, 13, 14, 24, 25).

Acquisition Program Baselines. Seven of the information technology acquisition reports noted incomplete or nonexistent acquisition program baselines. For example, the program office for the Joint Total Asset Visibility System had not established baselines for acquisition cost, schedule, and performance; therefore variances could not be calculated to determine if the system was being acquired in the intended manner. For the Composite Health Care System II, baselines had been established but evaluation was insufficient to determine whether program execution was within cost, schedule, performance and exit criteria parameters. In the case of the Corporate Executive Information System, the fact that it was not properly categorized as a MAIS led to the lack of established baselines. The Air Force Audit Agency found that the Airborne Information Transmission Program lacked the acquisition baselines necessary to measure program success. Without the establishment and continued evaluation of acquisition program baselines, it is difficult to determine if a system is being acquired in an efficient and effective manner (see Appendix B, reports 4, 12, 14, 16, 19, 24, 29).

Miscellaneous Recurring Problems. While not systemic, there were several other issues that appeared in three information technology acquisition reports. Testing was one of these issues. Both the Defense Civilian Personnel Data System and the Defense Security Assistance Management System lacked a Test and Evaluation Master Plan. Also, the GAO raised concern that the Army has not sufficiently tested its systems for the electronic warfare and information warfare threat. Testing is necessary to assure systems work properly and are properly protected against various threats (see Appendix B, reports 7, 14, 19).

The Corporate Executive Information System, the Defense Security Assistance Management System, and the Standard Procurement System experienced schedule slippages. Proper oversight and planning can minimize the instances of schedule slippages that usually result in increased costs (see Appendix B, reports 9, 14, 24).

Three systems were reported to have had faulty implementation strategies; the Defense Security Assistance Management System, the Defense Property Accountability System, and the DoD Electronic Mall. Without a proper implementation strategy, an otherwise well-functioning system may not be fully used and fielded to the appropriate users (see Appendix B, reports 3, 13, 14). The following matrix categorizes the weaknesses in the 30 reports that were reviewed.

Matrix of Information Technology Acquisition Weaknesses

Report No.	Inaccurate Cost Data/ Analysis	Inadequate Requirement Documents/ Validation	Wrong Acquisition Category	Inadequate Baselines	Inadequate Testing	Schedule Slip	Inadequate Implementa- tion Strategy	Inadequate Analysis of Alternatives
GAO								
NSIAD-00-56		X						
NSIAD-99-166					X			
AIMD-98-5	X	X						X
AIMD-97-6	X							X
IG, DoD								
D-2000-063								
D-2000-056	X						X	
D-2000-055	X		X	X				
00-027		X						
99-OIR-009			X					
99-220								
99-166	X	X				X		
99-068	X		X	X				
98-135		X	X				X	
98-095	X	X	X	X	X	X	X	
98-057				X				
98-041	X			X	X			
98-013								
97-206		X						X
97-205		X						X
97-152	X	X	X	X		X		
97-138		X	X					
ARMY AUDIT AGENCY								
AA99-147								X
AA99-87		X						
AA98-108								
AA97-53								
NAVAL AUDIT SERVICE								
016-98								
AIR FORCE AUDIT AGENCY								
97058036								X
96058037		X						X
96054009		X						X
96064027				X				

Conclusion

As illustrated in the 30 reports relating to DoD information technology acquisition issued from October 1, 1996, to March 31, 2000, DoD has yet to achieve its information technology functional area reform goal to institutionalize provisions of the Clinger-Cohen Act. The eight categories of acquisition weaknesses noted in this report are typical of areas that would be examined if a rigid acquisition oversight program existed. Because management controls were either not in place or not being followed, systems continued to be acquired by DoD whose full costs were not properly estimated, did not meet user needs, duplicated existing systems, and were not placed into the proper acquisition category.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is attempting to correct weaknesses in its acquisition of information technology by implementing a process of portfolio management oversight to better select the best mix of information technology investments to achieve mission outcomes. The effort by DoD to put in place the management controls necessary to adequately monitor the implementation of the Clinger-Cohen Act through the portfolio management process is intended to reduce the risk of further significant problems with the acquisition of information technology. Until a successful acquisition oversight process is fully implemented within DoD, efficient and economical acquisition of information technology will continue to challenge the DoD.

Appendix A. Audit Process

Scope and Methodology

Work Performed. This report summarizes DoD information technology acquisition weaknesses identified in 30 audit reports issued by the General Accounting Office and the Office of the Inspector General, DoD, from October 1, 1996, to March 31, 2000. GAO issued 4 such DoD information technology acquisition reports, IG, DoD, issued 17 reports, and the Service audit agencies released 9 such reports in the period chosen for review. The reports were analyzed to determine systemic weaknesses. A summary of each report is included in Appendix B.

DoD-Wide Corporate Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goals, and performance measures.

FY 2000 DoD Corporate Level Goal 2: Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure **(00-DoD-2)**.

- **FY 2000 Subordinate Performance Goal 2.4:** Meet combat forces' needs smarter and faster, with products and services that work better and cost less, by improving efficiency of the DoD acquisition process. **(00-DoD-2.4)**

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

  Performance Measure 2.5.3: Qualitative Assessment of Reforming Information Technology Management. **(01-DoD-2.5.3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

Information Technology Management Functional Area.

- **Objective.** Provide services that satisfy customer information needs. **Goal.** Improve information technology management tools. **(ITM-2.4)**

- **Objective.** Reform information technology management processes to increase efficiency and mission contribution. **Goal.** Institutionalize provisions of the Information Technology Management Reform Act of 1996. **(ITM-3.1)**

- **Objective.** Reform information technology management processes to increase efficiency and mission contribution. **Goal.** Institute fundamental information technology management reforms. **(ITM-3.2)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Defense Information Management and Technology high-risk area.

Appendix B. Summary of Prior Coverage

During the period of October 1, 1996, to March 31, 2000, the GAO issued 4 reports, the IG, DoD issued 17 audit reports, and the Service audit agencies released 9 reports on the topic of acquisition of information technology. The issues from these 30 reports are illustrated in a matrix on page 8. These 30 reports are summarized as follows:

1. General Accounting Office Report No. NSIAD-00-56, "Contract Management: Few Competing Proposals for Large DoD Information Technology Orders," March 20, 2000, OSD Case No. 1941. A review of 22 large information technology orders worth $533 million disclosed that the work descriptions for most of the orders defined tasks broadly. Because the work was broadly defined, the orders did not establish fixed prices for the work but provided for reimbursement of contractor's costs. Further, several broadly defined orders were later defined by sole-source work orders. It was recommended that DoD not award large, undefined orders and subsequently issue sole-source work orders for specific tasks. Management concurred with the recommendation.

2. Inspector General, DoD, Report No. D-2000-063, "Information Technology Funding in the Department of Defense," December 17, 1999. The FY 2000 budget submitted by DoD did not comply with House Appropriations Committee Report No. 105-591 direction to correct information technology funding inconsistencies. This occurred because guidance contained in DoD Regulation 7000.14-R, "DoD Financial Management Regulation," June 1998, addressing the funding of information technology systems, was inconsistent and provided broad exceptions. As a result, Operations and Maintenance appropriations, rather than Research, Development, Test, and Evaluation appropriations, were requested in the DoD FY 2000 budget submission for software modifications made to commercial off-the-shelf information technology systems, system solution definitions, software license acquisitions, and program support. As a corrective action, the Under Secretary of Defense (Comptroller) issued policy that will clarify procedures for funding information technology systems by requiring modernization efforts to be budgeted with Research, Development, Test, and Evaluation appropriations.

3. Inspector General, DoD, Report No. D-2000-056, "DoD Electronic Mall Implementation Planning," December 15, 1999. The Electronic Mall is a work in progress and updates are being made to improve its usefulness as a viable source of supply. However, management needed to address several implementation issues that were barriers to the Military Departments using the system including duplication of General Services Administration programs, development of metrics, and a system to measure the effectiveness of the Electronic Mall, possible duplication of payment of bank credit card fees, inadequate integrated comparison shopping system, and accuracy of cost recovery rate. Those unresolved implementation issues existed because the normal implementation planning process was not followed. Audit follow-up action is ongoing.

4. Inspector General, DoD, Report No. D-2000-055, "Acquisition Management of the Joint Total Asset Visibility System," December 14, 1999. The Joint Total Asset Visibility System program office did not establish sufficient management controls and appropriate oversight was not provided for the acquisition of the Joint Total Asset Visibility In-Theater and Global Automated Information Systems. As a result,

acquisition cost, schedule, and performance baselines were not established, variances were not computed to measure results, assess controls, and oversee acquisitions; and budget submissions were not verified and validated. Management responded by establishing an integrated product team.

5. Inspector General, DoD, Report No. 00-027, "Automated Systems Used to Prepare the Defense Logistics Agency Working Capital Fund Financial Statements," October 28, 1999. The Defense Logistics Agency and the Defense Finance and Accounting Service Center, Columbus, Ohio, did not adequately identify and evaluate critical accounting, finance, and feeder systems. Although limited reviews of the accounting and finance systems were performed, systems problems were not identified and fully documented. Additionally, the Defense Logistics Agency annual statement of assurance did not adequately reflect the effect that the system and related control deficiencies had on the ability to prepare financial statements. The Defense Logistics Agency did not define and evaluate the complete system architecture it used to capture the financial data to prepare the Working Capital Fund financial statements or the effort required to correct the deficiencies. Costly system modifications could result if the requirements are not considered when new systems are fully implemented. Management responded by reviewing the accounting and finance systems, coordinating a strategy to replace the systems, assigning specific responsibilities for corrective action, and identifying and evaluating all feeder systems.

6. Inspector General, DoD, Report No. 99-OIR-009, "The Joint Intelligence Virtual Architecture Program," September 3, 1999. Program Management provided a clear program vision and the program was on schedule towards achieving that vision. There were no apparent indications of weaknesses in the management of the program or financial resources. However, the system was not categorized as a MAIS, even though it meets the cost thresholds established to be categorized as such. The Director of the Program verbally agreed to bring the system into compliance with MAIS standards for requirements documentation, but the system is still not categorized as a MAIS.

7. General Accounting Office Report No. NSIAD-99-166, "Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort," August 11, 1999, OSD Case No. 1847. While the Army has carried out a number of tests of defensibility of digitized battlefield systems and forces, its protection plan did not assure sufficient vulnerability assessments. The Army lacked a detailed plan for specific systems, networks, and infrastructure for its information protection requirements. Without such specific plans, system vulnerabilities may not be exposed, adequate funding to counter the threat may not be available, and systems can be developed that do not meet the requirements of the Army's overall protection plan. The Army took corrective action by revising its information protection plan, reviewing and revising Operational Requirements Documents, and testing for susceptibility to electronic and information warfare threats.

8. Inspector General, DoD, Report No. 99-220, "Computer Equipment Acquisitions for the Defense Information Systems Agency Megacenters," July 21, 1999. This report addressed allegations that the Defense Information Systems Agency unnecessarily purchased new mainframe computers for its Megacenters. Specifically, the report addresses allegations that the prime contractor misled the government into purchasing new computer equipment rather than upgrading existing equipment. The constituent also alleged the Defense Information Systems Agency offered the

constituent's company a contract to maintain existing equipment under false pretenses. The allegations were not substantiated and the report contains no findings or recommendations.

9. Inspector General, DoD, Report No. 99-166, "Initial Implementation of the Standard Procurement System," May 26, 1999. The Standard Procurement System evolutionary software approach did not provide some critical functions to meet user needs or the mission need to replace legacy systems, and the program experienced schedule slippage. DoD may be required to obtain sole-source support for the system's 30-year life cycle. Thirteen of 25 fielded sites were not using the system because critical system functions that had been documented before system development were either not included in the system or not functioning. This occurred because DoD guidance on the acquisition of commercial products for MAIS was not clear; the Director, Defense Procurement, selected an acquisition strategy to purchase commercial computer software that required substantial modification; the acquisition strategy for this system of purchasing commercial computer software limited DoD rights to modify and maintain the software; and the Director, Defense Procurement, did not develop standard policies, processes, and procedures for using the system. Management agreed to issue guidance on these topics and will accept funds and requirements from users for coordination of added contract requirements. A follow-on audit of this system is ongoing.

10. Army Audit Agency Report No. AA99-147, "Digitization of the Battlefield: Tactical Internet," March 15, 1999. The requirements and testing approach for the Tactical Internet was generally effective for managing its development. The Army Audit Agency recommended that an integrated process team for examining options for funding digitization initiatives be established and a tactical internet requirements manager be appointed. Management agreed to implement the recommendations.

11. Army Audit Agency Report No. AA99-87, "Global Command and Control System-Army Program," January 22, 1999. The combat developer and the material developer did not adequately identify or satisfy user requirements for the Global Command and Control System-Army Program. The Army Audit Agency recommended that integrated concept teams be established to identify all user requirements and that the operational requirements document for the system be finalized and exit criteria be developed for developmental phases. Management agreed to implement the recommendations.

12. Inspector General, DoD, Report No. 99-068, "Acquisition Management of the Composite Health Care System II Automated Information System," January 21, 1999. Project management information for the system increments 1 and 2 was insufficient to determine whether program execution was within cost, schedule, performance, and exit criteria parameters. This occurred because the Assistant Secretary of Defense (Health Affairs) and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) did not establish acquisition baselines. Also, work breakdown structure linking financial accountability needed to be implemented to improve the ability to evaluate whether program results deviate from baseline parameters for costs, schedule, performance, and milestone decision authority exit criteria. Also, funding visibility for this system was limited as it was combined with funding for other systems. Management completed corrective action by instituting a project management control system to track and forecast costs, schedule, performance, and exit parameters and reconcile and validate results and conclusions

14

derived from program documentation. Also, management modified the Milestone II exit criteria to address auditor concerns and established the program with its own distinct funding line item.

13. Inspector General, DoD, Report No. 98-135, "Implementation of the Defense Property Accountability System," May 18, 1998. This system was developed to remedy a systemic weakness noted in the DoD Annual Statement of Assurance that DoD financial reporting of personal and real property was unreliable. The audit concluded that the system did not remedy that systemic weakness. The system has not captured all personal and real property, provided standard property reporting requirements, or developed a coordinated DoD-wide implementation strategy. At least $92 million may be spent on this system which, as designed, will capture barely 25 per cent of DoD personal and real property. To correct this situation, management revised its implementation strategy.

14. Inspector General, DoD, Report No. 98-095, "Defense Security Assistance Management System," March 24, 1998. This system was not being managed with controls appropriate to a system of its cost and size, and the program experienced schedule slippage. According to DoD Regulation 5000.2-R, any program with total life-cycle costs estimated to exceed $360 million should be classified as a MAIS. This system was not categorized as such, despite the fact that its estimated life-cycle cost is $500 million. For this system, a mission needs statement; an operational requirements document; a program baseline; an acquisition plan; and a test and evaluation master plan to assist in managing the cost, schedule, and performance parameters of the system were not prepared. Management has taken corrective action by preparing all of these documents; however, the program is still not classified as a MAIS. A follow-on audit of the system is ongoing.

15. Army Audit Agency Report No. AA98-108, "Corps of Engineers Financial Management System," February 13, 1998. Management controls over the Corps of Engineers Financial Management System were generally adequate to meet user needs and produce reliable and timely financial information. However, the Army Corps of Engineers needed to correct errors in its general ledger correlations and improve controls over specific individual expenditure authority for foreign military sales. The Corps made most of the suggested corrections during the course of the audit.

16. Inspector General, DoD, Report No. 98-057, "Defense Finance and Accounting Service Acquisition Program for the Electronic Document Management System," January 27, 1998. While there was no finding or recommendations per se, suggestions were made for improving this MAIS that were incorporated by the Program Office during the course of the audit. The suggestions were generally related to the establishment of baselines. The Program Office used the integrated product team approach to conduct testing, prepare life-cycle documentation, identify and resolve issues, and to make sound and timely suggestions to facilitate program decision-making.

17. Air Force Audit Agency Report No. 97058036, "Computer Upgrades and Random Access Memory Chips," January 9, 1998. The Air Force could improve management of computer upgrades and memory chips. Specifically, personnel could obtain computer upgrade kits rather than procuring new computers and procure memory chips through more economical methods. Also, personnel could enhance accountability and control of memory chips. Management concurred with the intent of

the recommendations and agreed that upgrading computers is a viable alternative to purchasing new computers. Also, local control procedures consistent with the Federal Acquisition Regulation will be established.

18. Naval Audit Service Report No. 016-98, "Acquisition of Computer Equipment and Displays on Air Force contracts," January 8, 1998. This report focused on the development and acquisition of Navy tactical computer and display equipment and systems on U.S. Air Force contracts via interagency fund transfers. The Naval Audit Service identified 12 projects totaling approximately $55 million that were being performed on Air Force contracts and funded by the Navy. Of this amount, $52 million was for three projects; therefore, this report focuses on those three projects. The audit concluded that Navy managers did not adhere to acquisition and appropriations policies and Congressional guidance concerning the development and procurement of shipboard tactical systems. The Navy also used Other Procurement, Navy and Ship Construction, Navy appropriations to fund development of new computers/displays that duplicate development of tactical display systems. Research, Development, Test, and Evaluation, Navy funds should have been used. Management generally did not concur with the finding or recommendations and the report was redirected to the Navy Office of the General Counsel for decision. The Office of the General Counsel required that some but not all recommended adjusting entries be made.

19. Inspector General, DoD, Report No. 98-041, "Acquisition Management of the Defense Civilian Personnel Data System," December 16, 1997. The Air Force had not established adequate management controls in this system's acquisition management structure to clearly define lines of responsibility, authority, and accountability as required by DoD Directive 5000.1, "Defense Acquisition," March 15, 1996. As a result, the Air Force could not ensure that it has adequately managed the high-level of risk associated with key areas such as testing, information assurance, and life-cycle costing. Management took corrective action to define lines of responsibility, authority, and accountability for the system's acquisition. Also, a program executive officer was appointed for the system, and management conducted a comprehensive in-process review of the program and instituted an integrated product team.

20. Inspector General, DoD, Report No. 98-013, "Second User Acceptance Test of the Electronic Document Management System at the Defense Finance and Accounting Service Operating Location Omaha, Nebraska" October 24, 1997. The Defense Finance and Accounting Service had resolved the functional deficiencies reported in the first user acceptance test. The system appears to be capable of performing, in an operational environment, the tasks assigned for the vendor payment process. The report contained no finding or recommendations.

21. General Accounting Office Report No. AIMD-98-5, "Defense IRM: Poor Implementation of Management Controls has Put Migration Strategy at Risk," October 20, 1997, OSD Case No. 1427. From 1995 through 2000, DoD planned to spend $18 billion on migration of outdated systems to modern systems. Despite this substantial investment, DoD did not adhere to decision-making and oversight processes it established to ensure that the economical and technical risks associated with migration processes have been mitigated. DoD did not fully ensure that economic analyses for migration systems were prepared and reviewed and that the systems comply with technical and data standards. By way of corrective action, management is updating migration policy to be consistent with the Information Technology Reform Act of 1996.

22. Inspector General, DoD, Report No. 97-206, "Defense Finance and Accounting Service Acquisition Strategy for a Joint Accounting System Initiative," August 22, 1997. The Defense Finance and Accounting Service developed an accurate and complete mission needs statement that demonstrated the need for an accounting system. During the course of the audit, Defense Finance and Accounting Service management addressed audit concerns by revising the mission needs statement to better present nonmaterial alternatives to the current systems; clarifying the effects of data from other systems on the projected benefits of a new accounting system; explaining more fully the customer's use of the system; outlining the use of the new system throughout DoD; recognizing the need for evaluating and improving business practices; and projecting the benefits to be achieved from implementing a new accounting system. However, subsequent audits raised additional concerns about acquisition planning for this system.

23. Inspector General, DoD, Report No. 97-205, "Dual Management of Commercially Available Items- Defense Logistics Agency Electronic Catalog Pilot Program," August 15, 1997. The Defense Logistics Agency was commended for starting an electronic catalog program from which customers may browse, select, and order commercially available items. However, portions of the program duplicated General Services Administration supply programs, particularly the Federal Supply Schedule and Advantage programs. Without programmatic change, there is no assurance that the system provides value to DoD. Also, customers ordering items through the electronic catalog could pay higher prices than if the same items were ordered through the General Services Administration. The Defense Logistics Agency efforts to increase sales through the electronic catalog did not include management controls to preclude commercial items that were not predominantly military and available from the General Services Administration. In essence, this was a failure to validate all system requirements to assure that aspects of the capability did not already exist. Management agreed to conduct a survey of customers to determine whether the electronic catalog should contain items that are commercially available through the General Services Administration.

24. Inspector General, DoD, Report No. 97-152, "Corporate Executive Information System," June 6, 1997. The system was not classified as a MAIS, and its life-cycle cost was not adequately estimated and reported. As a result, development risks, such as not meeting the needs of system users; slipping deployment schedules; incurring additional costs due to delays in the shutdown of existing systems; and the system not representing the best value solution for meeting user requirements were not mitigated. During the course of the audit, the Army Surgeon General Program Management Office transferred system approval authority to the MAIS Review Council. Because the system was reclassified during the audit as a MAIS, the additional controls associated with the new designation were deemed sufficient such that the report contained no recommendations.

25. Inspector General, DoD, Report No. 97-138, "Requirements Planning and Impact on Readiness of Training Simulators and Devices," April 30, 1997. DoD developed and procured large-scale computer training simulation programs without adequate control and oversight. As a result, DoD senior management has not received MAIS reporting and has not conducted milestone decision reviews for the large-scale training simulations. In addition, the Defense Advanced Research Projects Agency and the Joint Staff have investment plans to develop redundant, joint computer training

simulations. Also, the Army, the Navy, and the Air Force have not shown that large-scale computer training simulations are effective. Management took corrective action by establishing policy and strategy to better manage and oversee the acquisition of large-scale training simulation systems.

26. Air Force Audit Agency Report No. 96058037, "Automated Intelligence Information Systems Development," March 19, 1997. The Air Force did not adequately control development efforts, document the need, or obtain higher-level approval and subsequent funding for 6 of 12 automated intelligence information systems reviewed. Without validated needs and proper approvals, Air Force personnel could duplicate system capabilities of other Air Force or DoD activities. Also, the Air Force had not obtained approval to develop systems as migration systems. Independently developing systems without obtaining migration approval increases the possibility of stand-alone, noninteroperable systems that may not be effective during contingency operations. Management officials agreed with the overall results. The corrective actions taken or planned were considered responsive to the issues and recommendations. Corrective actions included nominating systems for migration status approval and discontinuing development of those systems not approved.

27. Air Force Audit Agency Report No. 96054009, "Combat Ammunition System," January 17,1997.   The Combat Ammunition System required additional controls to implement federal financial system control requirements and to correct modification and development efforts. Specifically, the system did not comply with 10 of the 17 mandated financial system controls. In addition, system modification and development efforts duplicated DoD system development. Further, Air Force management continued to modify and upgrade both the Air Force-level and command-level components even though DoD designated both as legacy systems. Management officials agreed with the overall audit results and planned to request waivers from the Corporate Information Management directives to continue their modification and upgrade initiatives. The management actions were considered responsive.

28. Army Audit Agency Report No. AA97-53, "Combat Service Support Control System," December 12, 1996. The combat developer generally identified user requirements for combat service support. The Combat Service Support Control System was being developed to satisfy most combat service support requirements. However, material and combat developers needed to improve processes to make sure remaining requirements were satisfied. Management undertook corrective action during the audit.

29. Air Force Audit Agency Report No. 96064027, "Airborne Information Transmission Program," November 29, 1996. The Air Force did not follow existing policy and direction in executing the subject program. The Airborne Information Transmission Program acquisition managers did not establish exit criteria for the current program acquisition phase. Also, the program manager did not prepare an acquisition program baseline to establish cost, schedule, and performance thresholds. As a result, program management did not have well-defined goals and objectives to manage and measure program progress. Management took satisfactory corrective action including proposing a set of exit criteria and acquisition program baselines.

30. General Accounting Office Report No. AIMD-97-6, "Defense IRM: Strategy Needed for Logistics Information Improvement Efforts," November 14, 1996, OSD Case No. 1219. Continued deployment of information systems by DoD using a migration strategy for the depot maintenance, material management, and transportation business areas will not likely produce the significant improvements originally envisioned. DoD continued to deploy information systems that are linked to the same business functions it wishes to make more efficient and economical through outsourcing and privatization. DoD has not taken the fundamental steps necessary to ensure that the automated systems it deploys will yield a positive return on investment. Management took corrective action by creating a Strategic Information Resources Plan.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Under Secretary of Defense (Acquisition, Technology and Logistics)
Assistant Secretary of Defense (Command, Control, Communications, and
    Intelligence)
  Deputy Chief Information Officer, Office for Investment and Acquisition
Deputy Under Secretary of Defense (Acquisition Reform)
Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff
  Director, Command, Control, Communications, and Computers

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Chief Information Officer
Auditor General, Department of the Navy
Superintendent, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Resource Management, Defense Commissary Agency
Inspector General, Defense Intelligence Agency
Defense Systems Management College

Non-Defense Federal Organizations

Office of Management and Budget
  National Security Division
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
  Relations, Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
  Committee on Government Reform.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas Gimble
Mary Lu Ugone
Charles Santoni
John A. Mitton
Jenshel Marshall